**International Journal of Computer Networks and Distributed Computing**
***Vol. 4, Issue 2***

# Detection Strategies and Network Intrusion Detection Techniques for DDos Attacks

**Meshei.l [1] , Clueer Lopeuien[2]**

PG Scholar, Dept. of CSE, S.A Engineering College, Chennai, Tamil Nadu, India[1]

Assistant Professor, Dept. of CSE, S.A Engineering College, Chennai, Tamil Nadu, India[2]

ABSTRACT: **Some of the most exciting attacks done on networks today are those that are difficult to track, and requires very minimal effort on the attacker's part. Denial of Service (DoS) has the most destructive effects among the various online attacks which is hindering the security. The security experts are in tremendous pressure, to bring out effective defence solutions for the various attacks occurring recently. Variety of tools and coding are used to implement these destructive attacks. DoS attack has managed to exist in the internet for more than a decade as there is no steady solution to prevent this attack. The Intrusion prevention system is used as an extension of Intrusion detection system as a prevention technique for the DoS attacks. Network Intrusion Detection and Prevention system analyzes the packets coming and going through the interface. The paper provides the idea of various types of DoS attacks, detecting them and preventing them. There are many methods which are available to detect and resist the DoS attack. The detection and prevention techniques shown are effective for small network topologies and can also be extended to analogous large domains.**

**Keywords: Denial of Service (DoS), Distributed Denial of Service, IDS (Intrusion Prevention System), IPS (Intrusion Prevention System), NIDS (Network Intrusion Detection System)**

## I. INTRODUCTION

Denials of service (DoS) attacks pose an immense threat largely to the Internet and also the network systems and many defence mechanisms have been proposed to overcome the problems. Attackers try constantly to modify their attack methods to surpass the security systems and researchers in turn modify their approaches to handle such attacks. The DoS attack is becoming more and more complex now a day. There is variety of known attacks which creates the impression that the problem space is more, and hard to explore. The existing systems employ various techniques to counter the problem, and it is difficult to understand their similarities and differences and to evaluate their effectiveness and cost.

Denial of Service is an attack which makes an information or data unavailable to its intended hosts. This attack can be carried out in various ways and various strategies are mentioned. The underlying aspect would be to congest victim's network and thus make it inaccessible by other client. There are many other ways of making service unavailable rather than just flooding it with abundant IP packets. The victim could also be attacked at various loopholes making it unstable which depends on the nature of the attack.

There are many manifestations of Denial of Service attacks but they ultimately have the same objective that is to deny or degrade users' ability to legitimately access network. DoS attacks are accomplished by draining the limited resources of network bandwidth by flooding with packets or exhausting host resources by consumption of CPU cycles, random memory, static memory or data structures .DoS attacks can generally be classified as either a Flood Attack or a Malformed Packet Attack and that where attacks originate simultaneously from several compromised sources that these can be classified as Distributed DoS attacks.

## II. OVERVIEW OF DOS ATTACKS

Denial of Service is an attack which makes an information or data unavailable to the legitimate hosts. The victim could also be attacked at various loopholes making it unstable which depends on the nature of the attack. There are many types of attacks crafted specially for networks like Congesting network resources, Draining CPU memory cycles, Reducing computing power and Poisoning domain name translations.

There are attacks that are carried out at application level, hindering the normal functioning of a service. There are attacks that crash web browser, email application or even a media player. When a specific application is disrupted and when normal functioning is hindered, it is called the Application level Denial of Service.

As a worst case, there are attacks that can cause permanent damage. These kinds of attacks are called the Permanent Denial of Service or Phlashing. Permanent Denial of Service attacks are mostly network based firmware updates and it aims to make the hardware inoperable. Firmware is the inbuilt code or program that is embedded on every electronic system for its proper functioning. When an attacker changes the firmware and replace it with a defective or corruptive code, the hardware could no longer be used. These attacks could be

directed towards networking components like routers, switches or bridges and thus bringing an entire routing table to collapse. A fault in a single router might lead to a huge outage if it does not have enough backups and rerouting. Often devices, who try to upgrade their firmware online without checking for the signature of a trusted source, will fall prey for this attack.

## III. DOS ATTACK MECHANISM

Denial of service attacks can be further classified into many categories according to the style with which it is implemented.

### *A. Distributed Denial of Service*

The most stunning feature of the DDOS attack was that it appeared to emanate from multiple sources, not all of which were obviously directly owned or controlled by malicious parties. The first stage of this attack is to build its platform with many host systems that can work under remote commands. The attacker first scans the networks to hunt for vulnerable systems that are weak in security features. The compromised systems which are termed as zombies will be infected with relatively sophisticated software called as DDoS clients.

The programs used to remotely control compromised zombies have been termed bots (after robot) because they typically rely heavily on remote automation techniques borrowed from Internet Relay Chat (IRC) scripts of the same name. A group of zombies under the control of a single entity is called a zombie network or bot army. The controlling entity can directly bombard a target computer or network with a SYN flood or other DoS attack. Fig.1 shows a simplified diagram of a DDoS attack using a single zombie network.

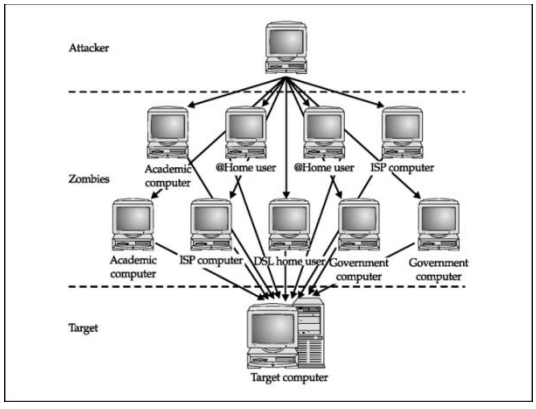


Fig.1: Single Zombie performing DDoS attack

Special root kits are also used where they are installed in a host system to incur these software exploitations. After having sufficient hosts under control, attackers also create backdoors that allows special access that is used for future entry.

### *B. Low Rate TCP Targeted DoS Attacks*

The attacks called the Shrew attacks are carried out by exploiting the TCP timers. This attack uses a low rate burst designed to exploit TCP's retransmission timeout mechanism, throttles the bandwidth of a TCP flow in a stealthy manner. When there is congestion in TCP network, the congestion window is gradually reduced until the network is clear. Thus during congestion the sender's rate is reduced which apparently reduces the potential throughput. The TCP waits for the Retransmission Time out (RTO) to expire after which the data is sent again. When the congestion is more in the network, the RTO timer is doubled after which the packets are retransmitted. Thus during a low rate attack, when packets are lost, TCP enters RTO. When an attacker is able to calculate this RTO time, the attacking packets are sent to create packet collision and loss thus pushing the TCP into waiting state.

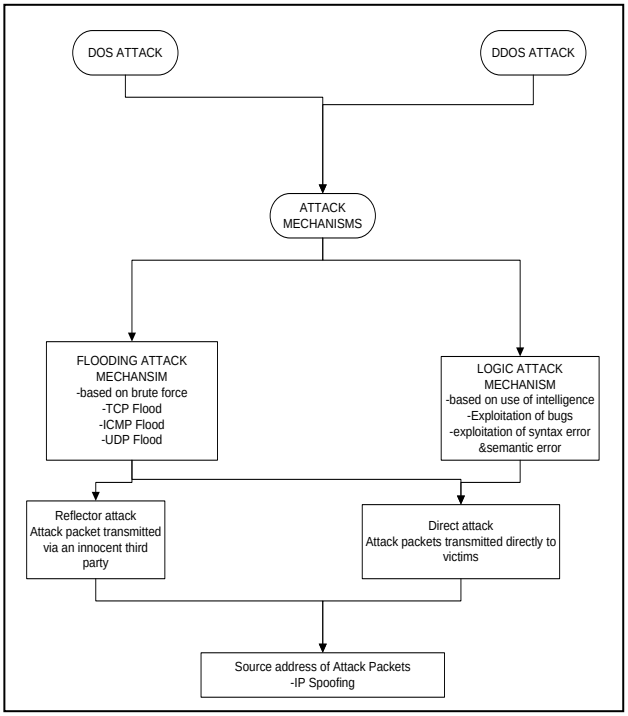


Fig.2 Attack mechanisms by DOS and DDOS

Fig.2 shows the various attack mechanism by the denial of service attacks and the distributed DoS attacks.

## IV. TYPES OF DOS ATTACKS

There are several flavours of Denial of Service that could disrupt a normal service. The attacking methods are classified into two methods.

- First type would be to flood the network not leaving enough bandwidth for the legitimate packet which is termed as Flooding.
- The other method is to crash a hardware or software and make it inoperable. Web servers, routing devices, DNS look up servers are the common targets that could be crashed during an attack.

### *A. Ping of Death*

Ping of death is caused by an attacker sending a ping packet (normally 64 bytes), that is larger than the 65,535 bytes. Computer systems cannot handle an IP packet that is larger than the maximum IP packet size, and leads to crashing of computer systems. A packet of larger size can be sent if it is fragmented. When a receiving computer system reassembles the packet, a buffer overflow occurs, which leads computer to crash.

### *B. Ping of Flood*

Ping of flood is caused by an attacker overwhelming the victim's network with ICMP Echo Request packets. This does not require extensive network knowledge as many ping utilities support this operation. Ping flood traffic consumes significant bandwidth on low to mid-speed networks bringing down a network to a crawl.

### *C. Smurf Attack*

Smurf attach exploits the target by sending repeated ping request to broadcast address of the target network. The ping request packet often uses forged IP address , which is the target site that is to receive the denial of service attack. The result will be lots of ping replies congesting the spoofed host. The network will not receive real traffic if the number of hosts replying to ping request is large.

### *D. SYN Floods*

When establishing a session between TCP client and server, a hand-shake message exchange occurs between a server and client. A session setup packet contains a SYN field that identifies the sequence in the message exchange. An attacker may send a flood of connection request and do not respond to the replies, which leaves the request packets in the buffer so that legitimate connection request can't be accommodated.

### *E. Teardrop Attack*

Teardrop attack exploits the network by sending IP fragment packets that are difficult to reassemble. A fragment packet first identifies an offset that can be used to assemble the entire packet so that the receiving system can reassemble them. In this attack, the attacker's IP puts an offset value in the subsequent fragments that confuses the receiving system thus making the system unable to handle that situation in turn leading to system crash.

### *F. Mail Bomb*

This is the denied email service to the legitimate users when the unauthorized users send large number of email messages which has large attachments to a particular mail server thus filling up disk space.

## V. IDS AND IPS OVERVIEW

An Intrusion Prevention System (IPS) is extension of Intrusion Detection System (IDS) which is the combination of Intrusion Detection System and Firewall. The IDS and IPS together provide a better network security solution. The IDS captures data packets in real time, processes them to identify the threats and responds to the attack. This works only on copy of data traffic and mainly uses the signature to detect the suspicious activity. This is referred to as promiscuous mode. On the other hand IPS works inline in data stream to provide protection against the attack traffic. This is called as inline mode.IPS does not allow malicious traffic to enter the trusted area of the network but IDS the traffic to pass through the network and only then responds.

### *A. Intrusion prevention system(IPS)*

An Intrusion Prevention System uses highly sophisticated and dedicated technology to provide increase levels of protection against DoS and Network Worm type attacks.

The majority of intrusion prevention systems use one of three detection methods:

- Signature-based,
- Statistical anomaly-based,
- Firewalls
- Policy based and
- Honey pot based.

#### *1) Signature-based Detection:*

This method of detection makes use of signatures, which are attack patterns that can be preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic to match with the signatures which are preconfigured and stored in a database. If a signature matches the intrusion prevention system takes the appropriate action. The signature database has to be constantly updated because of the various new attacks whose signature cannot be identified in detection.

Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyse patterns appearing in exploits which are being protected and vulnerability-based signatures analyse vulnerabilities in a program, its execution, and conditions needed to exploit.

#### *2) Statistical Anomaly-based Detection:*

Anomaly detection or profile based signature monitors the network traffic that deviates from the normal traffic. A baseline is created, and the system intermittently samples network traffic, using statistical analysis to compare the sample to the already set baseline. If the activity deviates from the baseline parameters, the intrusion prevention system takes the appropriate action.

*3) Firewalls*

Firewalls are a form of Intrusion Prevention System. The main purpose of the firewall within the Enterprise is to enforce Enterprise policy and maintain connection state information for legitimate users internally or externally and not to prevent high volume DoS / DDoS style attacks.

*4) Policy Based Detection:*

In a policy based detection system, a predefined set of security policies are created. Any network traffic which is detected outside the security policy will generate an alarm or drop off from the network. The policy must be designed with a detailed knowledge of the network traffic.

*5) Honey-pot based System:*

This uses a dummy server to attract attacks towards the network. This helps to distract attacks from real network devices. These types of systems are mainly used in production environment and large organizations which come across as targets for attackers.

*B. Intrusion detection system(IDS)*

Intrusion detection is a set of methods that are used to detect suspicious activity both at the network and host level. Intrusion detection systems fall into two basic categories:

- Signature-based intrusion detection systems and
- Anomaly detection systems.

*1) Network IDS or NIDS:*

NIDS are intrusion detection systems that capture data packets travelling on the network media and analyze them. The data packets are then matched with the signature in the database. If the packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database.

*2) Host IDS or HIDS:*

Host-based intrusion detection systems are installed as agents on a host system. These intrusion detection systems can look into host system and application log files to detect any intruder activity. Some of the systems informs when something malicious activity happens, such systems are said to be reactive. Some systems are proactive; the systems can sniff the network traffic coming to a particular host on which the HIDS is installed and alerts in real time.

Fig.3 shows the methods to detect the types of DoS attacks. To detect the attacks or malicious traffic on the network first step is to capture the packets. There are two modes present to capture the packet one is normal in that the packets intended to the system are only captured by the system. And other is promiscuous mode in which every packet which is going through the interface is captured by the system. So to monitor the network traffic the system has to be operated in promiscuous mode.

The overall architecture contains the following units.

1. **Packet Sniffer unit**: This unit captures the packet from the network interface either in promiscuous mode or in normal mode.
2. **Intrusion Detection or Pre processing engine**: In this unit it uses the different approaches to detect the attack depending on flow based analysis or protocol based analysis.
3. **Countermeasures**: In this, the packet which contains the malicious code are identified or if any abnormal flow of packets is observed then the particular action is selected to avoid the intruder to enter in to the network.

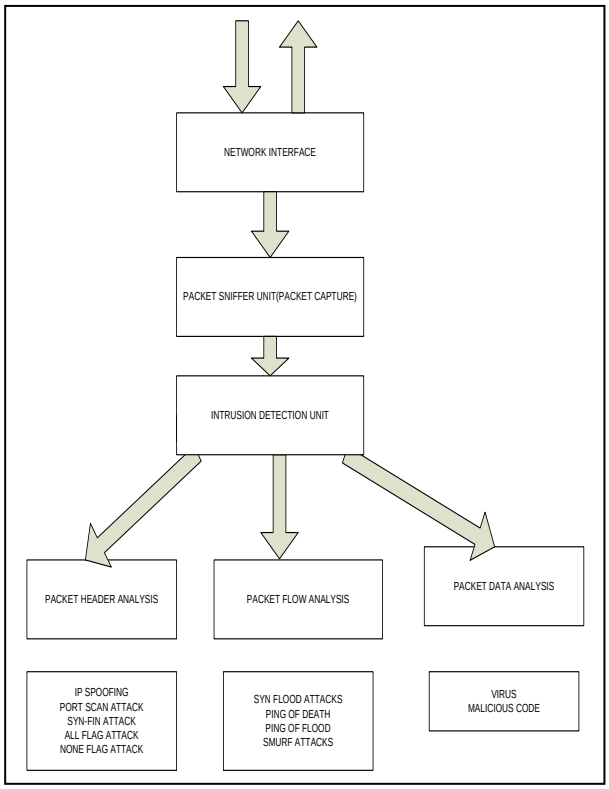


Fig.3: Types of DoS attacks detected

## VI. CONCLUSION

This paper gives adequate knowledge on various Denial of Service and DDoS attack mechanisms and also various

types of DoS attacks in the network. It also suggests basic mitigation strategies that could be adopted in order to defend attacks. The DoS attacks are detected by analysing of incoming packet and outgoing packets. The outline of various Intrusion detection and Intrusion prevention techniques are discussed. The methods to detect the DoS attacks in the network are discussed.

**Acknowledgement**

I would like to express my gratitude to my Internal guide Mr. C.Balakrishnan M.E (PhD), and coordinator Mr. Muthukumaraswamy M.E, Department of PG Studies, without their guidance, this would not be possible. I also wish to record my thanks to our Head of the Department Mrs.Umarani Srikanth M.E (PhD) for her consistent encouragement and ideas.

## REFERENCES

[1] Subramani Rao, Sridhar Rao, "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis", SANS institute Infosec Reading Room Sep 11,2011.

[2] Suchitha Patil, Dr.B.B. Meshram, "Network Intrusion Detection and Prevention Techniques", International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012

[3] Adrian Brindley,"Denial of Service attack and Emergence of 'Intrusion prevention system' ", SANS institute Infosec Reading Room,Nov 1,2002.

[4] Cheung, S.; , "Denial of service against the Domain Name System," Security & Privacy, IEEE , vol.4, no.1, pp. 40- 45, Jan.-Feb. 2006

[5] X.Geng and A.B.Whinston,"Defeating distributed denail of service attacls",IT Professional,vol 2,no4, pp.36-42 july-aug2000

[6] Fred Halsall " Computer Networking and Internet", 5th Ed., South Asia:Doring Kindersley.pp 6-31.

[7] E. Earl Eiland, Scott C. Evans, T. Stephen Markham, Bruce Barnett, "Network Intrusion Detection: Using Mdlcompress For Deep Packet Inspection",2008 IEEE

[8] Shikha Goel , Sudesh Kumar , "An Improved Method of Detecting Spoofed Attack in Wireless LAN", 2009 First International Conference on Networks & Communications 2009 IEEE

[9] Hui Li, Dihua Liu , "Research on Intelligent Intrusion Prevention System Based on Snort", 2010 Intern ational Conference on Computer, Mechatronics, Control and Electronic Engineering.

[10] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage. Inferring internet denial-of-service activity. *ACM Trans. Comput. Syst.*, 24(2):115–139, 2006.

[11] Carl Endorf, Eugene Schultz and Jim Mellander, "http://searchsecurity.techtarget.com/feature/The-future-of-intrusion-detection-and-prevention" from book Intrusion Detection and Prevention.

[12] Aaron Weiss,http://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html[Online] Available